Rambus

Implementing Strong and Programmable Security to Mitigate IoT Threats

Track: 268-TU867

Steve Singer

Sr. Director, WW Field Applications Engineering

ssinger@rambus.com

Boston, MA

617.823.8553

June 4th, 2019

Design Automation Conference

Las Vegas Convention Center

Rambus at a Glance

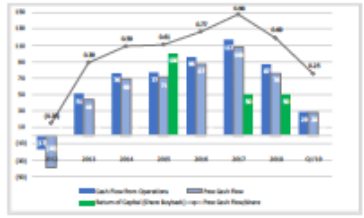
Rambus Offerings

Architecture Licenses	High-speed IO & DPA Countermeasures
IP Cores	Memory & SerDes PHYs; Secure Cores
Chips	Memory Buffers for DIMM modules
Key Management	Secure Supply Chain Provisioning

Financial Performance

Royalty	$24.9M	License Billings	$75.5M
Product	$9.0M		
Contract	$14.6M	Royalty	$24.9M
Revenue	**$48.4M**	**Delta**	**$50.6M**

Cash from Operations
Q119: $28.8M



NASDAQ: RMBS

25+ Years
Tech leadership & innovation

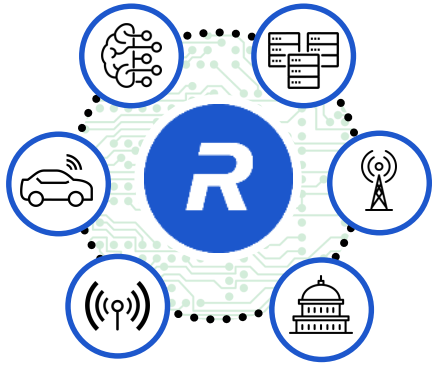
2500+
Patents and Applications

HQ: Sunnyvale, CA
WW Offices in India, EU, Asia

~800
Employees Worldwide

Rambus Security Products

Solutions to protect devices from birth to decommission



Source Code RTL

STD/DPA Cores & Test Equipment

Encryption Ciphers

Source Code RTL

Root of Trust Core

Platform Security

Provisioning Appliances

Key & Asset Injection System

Key Management Service (KMS)

Device Lifecycle Mgmt

End to End Security Solution

Presentation Focus

IoT Security Research Study

Analyzed IoT devices from manufacturers of:

- TVs
- Webcams
- Home thermostats
- Remote power outlets
- Sprinkler controllers
- Door locks
- Home alarms
- Garage door openers
- Hubs for controlling multiple devices

- A majority of devices included some form of cloud service
- 70% of the most commonly used IoT devices contain serious vulnerabilities
- 70% of devices used unencrypted network service
- 25 vulnerabilities were found per device on average

IoT Attacks on the Rise

NEWS

Chinese firm recalls camera products linked to massive DDOS attack

Hangzhou Xiongmai Technology is recalling earlier models of four kinds of cameras due to a security vulnerability

Source: http://www.pcworld.com/article/3133962/chinese-firm-recalls-camera-products-linked-to-massive-ddos-attack.html

SF Muni Hack a Wake-Up Call for Public Systems

By Richard Adhikari
Nov 28, 2016 3:28 PM PT

Fare payment machines at underground stations were out of order, resulting in free rides on the subway and light rail system known locally as "SF Muni."

Source: http://www.technewsworld.com/story/84112.html

The FTC has sued D-Link over unsecure routers and webcams

Part of an ongoing effort to secure the Internet of Things

by Andrew Liptak | @AndrewLiptak | Jan 7, 2017, 1:00pm EST

Source: http://www.theverge.com/2017/1/7/14199232/ftc-sued-d-link-unsecure-routers-webcams-cybersecurity

Foscam Security Cameras Full of Security Flaws

by **PAUL WAGENSEIL** Jun 8, 2017, 8:48 AM

We've said it before, and we'll say it again: Don't buy cheap Chinese-made security cameras, because their security may just be terrible.

Source: http://www.tomsguide.com/us/foscam-camera-flaws,news-25254.html

Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks

Russian hackers may be behind attacks leveled at the nation's power grid and artillery. The West should take note.

DHS Releases Strategic Principles For Securing The Internet Of Things

Release Date: November 15, 2016

Source: https://www.dhs.gov/securingtheIoTits

Connected Device Threat Landscape

- Connecting devices opens a wide range of new attack vectors
- Compromise of connected devices can have serious consequences
- Connected devices need strong security

Privacy
Tap security cameras or baby monitor video stream

Repurpose
Device is repurposed to be used in a botnet

Sabotage
Reprogram an appliance firmware to cause a failure

Vandalism
Control an IoT device to cause property damage

False Alarm
Initiate false alarm from smoke detector or security system

Physical Security
Disable the burglar alarm, unlock your front door

Trojan
Used to attack other devices in your home network

Infrastructure
Distributed attack to bring down the power grid

Meltdown/Spectre/Foreshadow Exposed Hardware Exploits

General Purpose Computing

- Always a **tradeoff of performance, area, power, and cost** with security being the compromise

Example attacks:

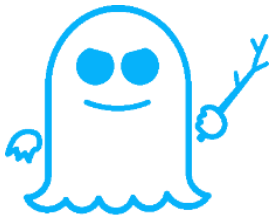
- CPU data **cache timing attack** to efficiently exploit and leak information out of the system
  - Manifested by **Speculative & Out of Order Instruction Execution**

Rambus Security Research:

- Security researchers Paul Kocher and Mike Hamburg contributed to the Spectre discoveries that impacted Intel, AMD, and ARM CPUs

Takeaway?

→ ***Sensitive security functions need to be run in a separate siloed processing core!***



SPECTRE

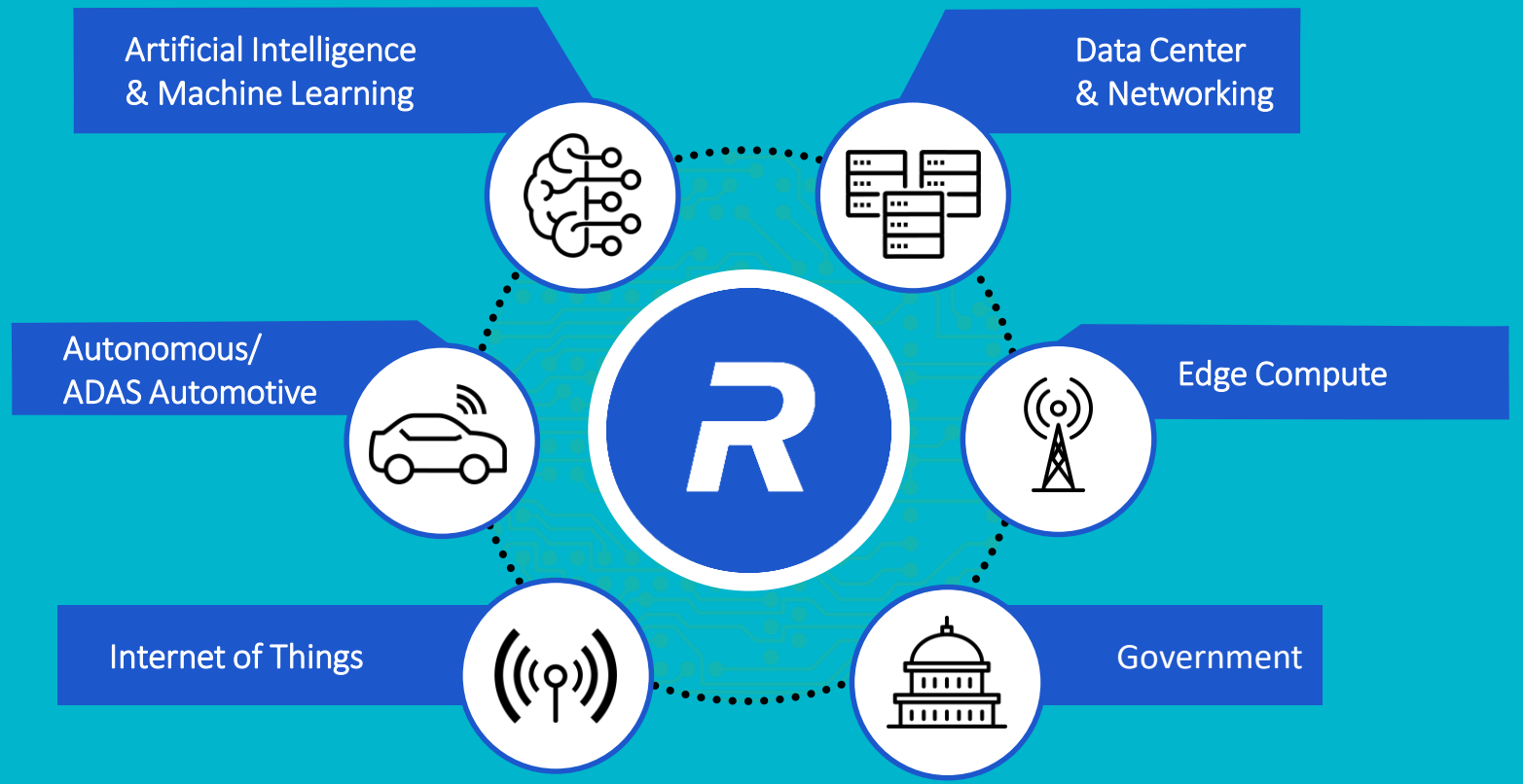
MELTDOWN

FORESHADOW

*Image credit to www.meltdownattack.com

CryptoManager Security Platform

Embedded Hardware Roots of Trust

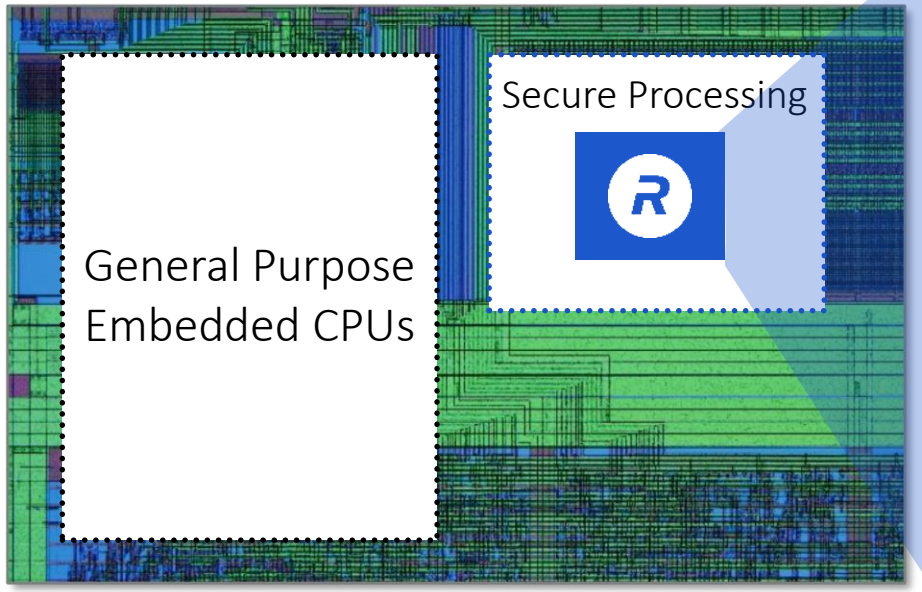


Rambus

Data · Faster · Safer

CryptoManager Root of Trust – "Secure Island in Silicon"

Complimentary to Main CPUs to Anchor Platform Trust



CryptoManager Root of Trust

Custom RISC-V CPU

Secure Memory

Secure Functionality:

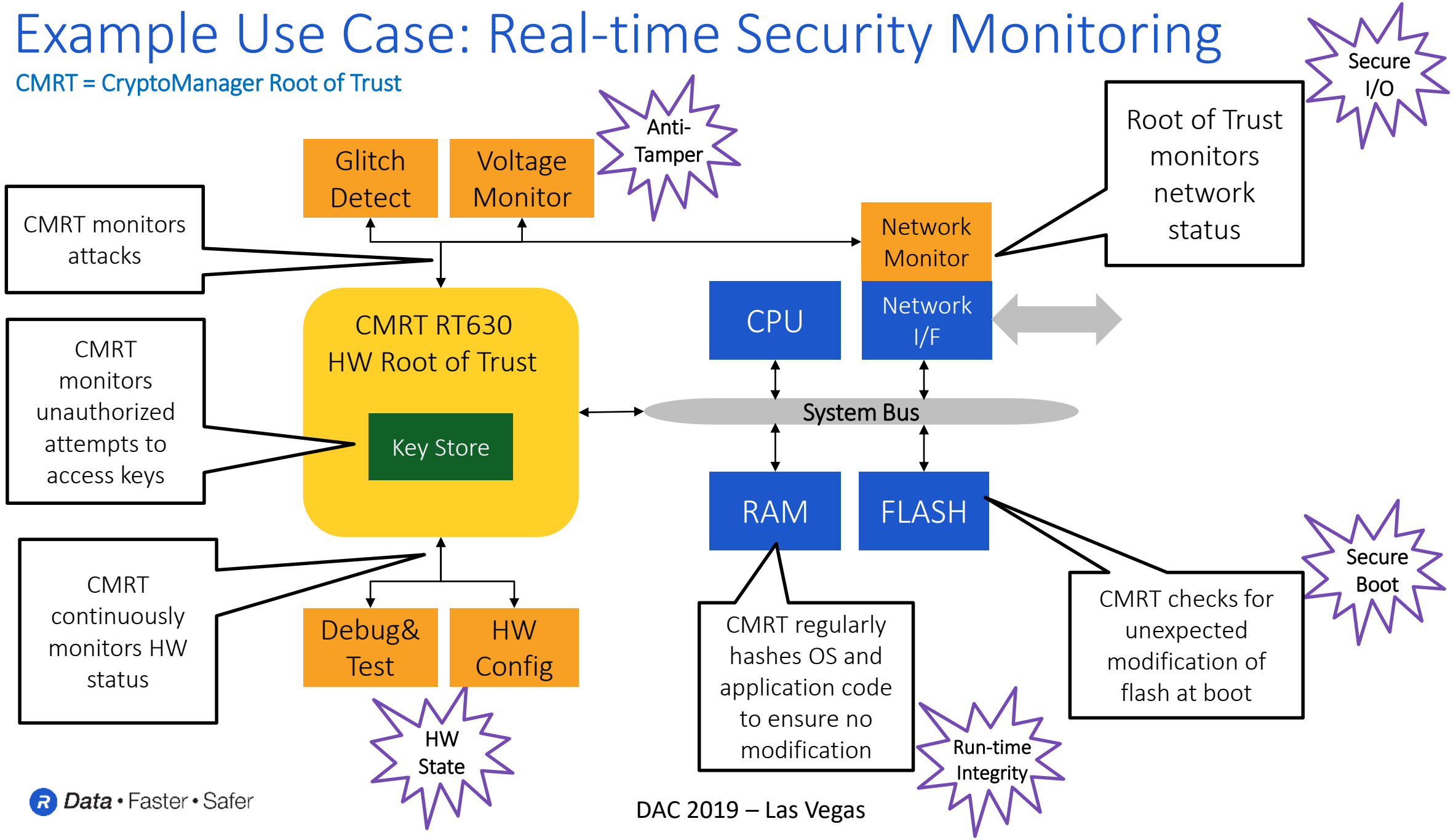
- Secure boot
- Secure IDs
- Secure communication
- Runtime integrity
- Etc.

Crypto Accelerators
(AES, SHA, others…)

A secure Root of Trust that provides a foundation for security throughout the SoC

Example Use Case: Real-time Security Monitoring

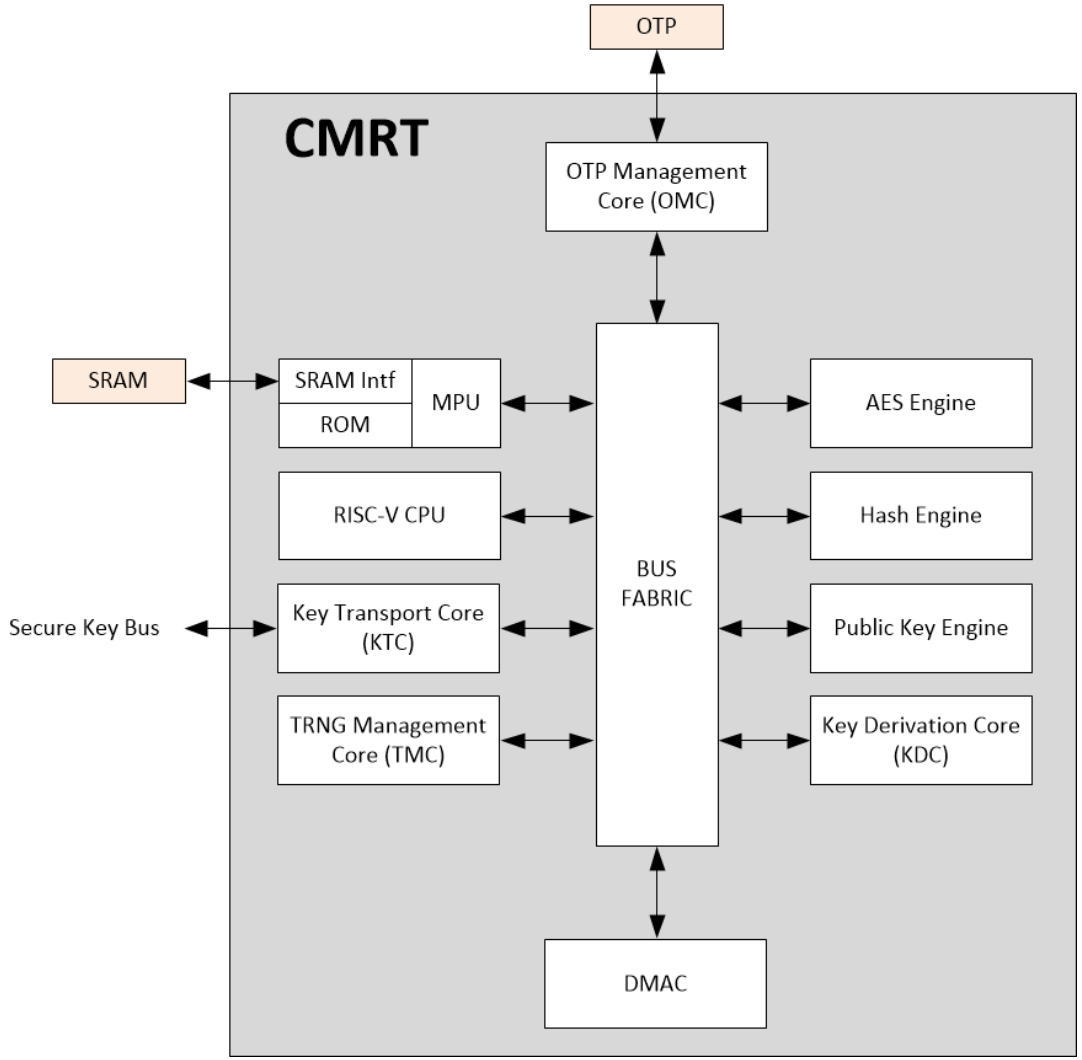
CMRT = CryptoManager Root of Trust



CryptoManager Root of Trust Block Diagram

A secure processor-based, software programmable Root of Trust (RoT) delivered as **Verilog RTL for ASIC and FPGAs**:

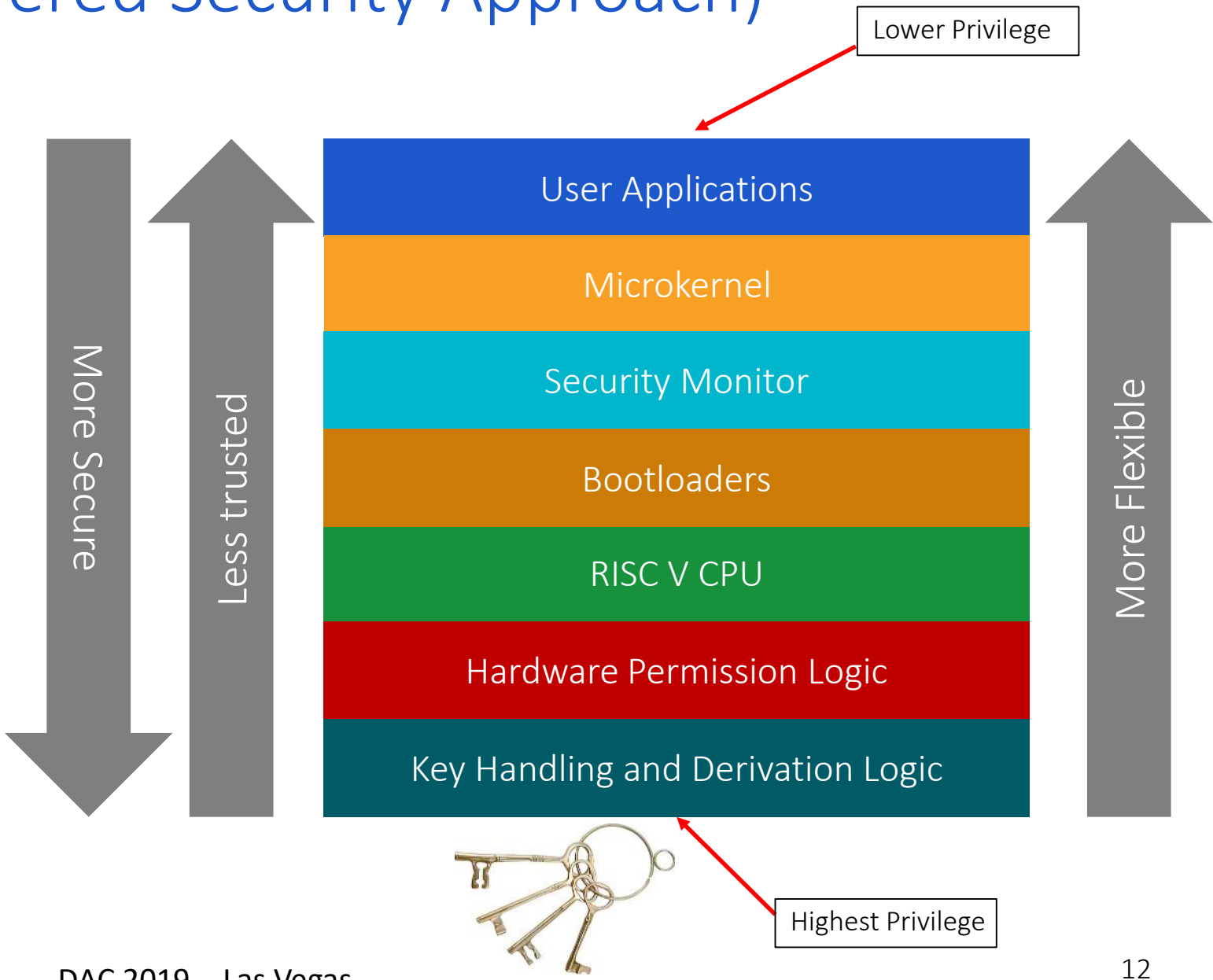
- Provides **full suite of security services** to main CPU such as **secure boot, secure runtime integrity, and remote attestation, and broad crypto acceleration**
- **Embedded RISC-V CPU** enabled 3rd-party application development within trust boundary
- **Modular architecture** to balance performance verses area
- Software based cipher algorithms can be updated post-silicon to support future cryptography requirements
- A **secure location** that **stores and manages security assets** such as keys and certificates
- HW-enforced security firewall (i.e. - permissions) enforces access rights
- **Tamper detection and resistance to side-channel attacks**



CMRT diagram is simplified

Defense in Depth (A Layered Security Approach)

- The attacker only needs to find the weakest link in the chain
- No single, point security implementation is resistant to all security attacks
- Therefore, a secure but rigid foundation is required where security critical operations are hardened while still allowing programmability as security threats evolve

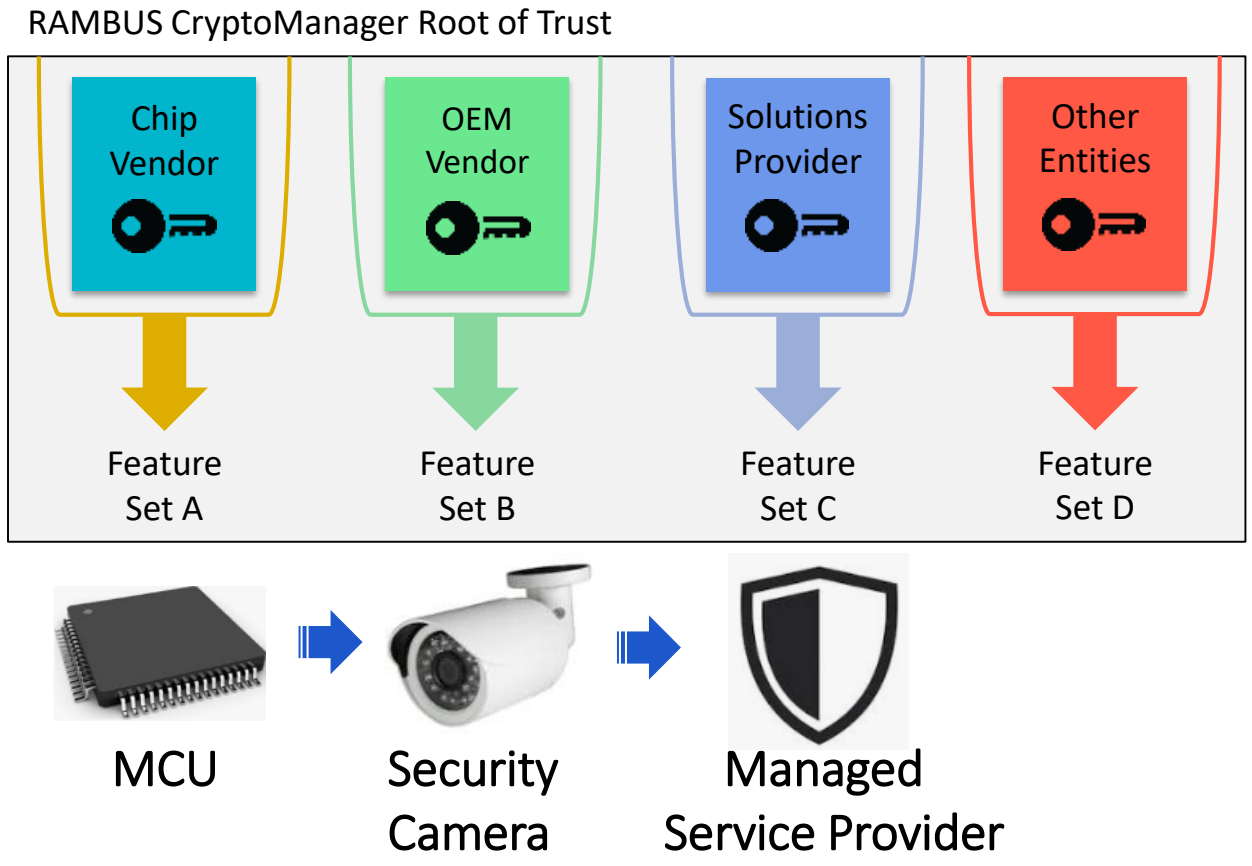


Running Isolated Roots Within a Single Security Subsystem

Multiple apps need to run in the security processor and come from different root entities

Unless these apps are isolated from each other and provide specific levels of security access, rogue apps can spread and infect others

CryptoManager Root of Trust allows the chip vendor and device OEMs to assign multiple roots supporting the entire device lifecycle



Hypothetical Use Case: Home Security - (Unique Device ID's, Keys and Firmware)

CryptoManager Root of Trust Use Case Summary

Programmable hardware Root of Trust enables a wide range of use cases

- Secure booting of system SW
- Run-time integrity of system SW
- Secure system monitor
- Secure firmware updates
- Device personalization (Unique device keys and IDs)
- Key and data provisioning
- Secure data storage
- Secure key storage
- Authentication (Local and Remote)
- Attestation (SW & HW states, SW update confirmation)
- Secure communication (TLS, MKA/MACsec, etc.)
- Cryptographic algorithm acceleration (AES, SHA, RSA, etc.)
- Secure debug / RMA
- Feature/Configuration/SKU management
  (Example: Enable Features in Field)

Thank You!

CryptoManager Platform

https://www.rambus.com/security/cryptomanager-platform/

CryptoManager Root of Trust

https://www.rambus.com/security/cryptomanager-platform/root-of-trust/

CryptoManager Infrastructure

https://www.rambus.com/security/cryptomanager-platform/cryptomanager-infrastructure

Rambus

Data · Faster · Safer